IN THE CLAIMS

1. (currently amended) An information processing apparatus for ~~transmitting~~ carrying out secure transmission of content to another apparatus ~~via~~ over a network, said information processing apparatus comprising:

an encryption unit operable to encrypt the content;

an authentication unit operable to ~~perform an~~ receive authentication ~~procedure with~~ information from the another apparatus when the another apparatus requests permission to receive the encrypted content, and to determine whether the authentication information is valid~~, said authentication procedure providing an authentication result~~;~~a transmitter operable to transmit a decryption key for decrypting the encrypted content to the another apparatus based on said authentication result;~~

a first obtaining unit operable to obtain identification information of the another apparatus ~~based on said~~ from the authentication~~ result~~ information when the authentication information is valid and to determine whether the identification information of the another apparatus is already stored in a storage unit;

a transmitting unit operable to transmit a decryption key to the another apparatus when the authentication information is valid, the decryption key being needed to decrypt the encrypted content; and

a first counting unit operable to increment a count of a total number of apparatuses ~~units desiring~~ to receive the encrypted content ~~based on said~~ by one when the identification information of the another apparatus is not already stored in said storage unit and the count of the total number of apparatuses is less than a maximum value;

said ~~a~~ storage unit being operable to store ~~said~~ the identification information of the another apparatus when the identification information of the another apparatus is not already stored in said storage unit~~; anda controller operable to control a total number of units approved to receive the encrypted content based on said total number of units desiring to receive the encrypted content~~.

2. (currently amended) An information processing apparatus according to Claim 1, wherein the another apparatus is operable to transmit the encrypted content to a plurality of further apparatuses over the network, and said information processing apparatus further comprises~~ing~~:

a second obtaining unit operable to obtain a first value and a second value from the another apparatus when the authentication information is valid, the first value being a number of apparatuses in the plurality of further apparatuses ~~additional units desiring~~ that are newly requesting to receive the encrypted content, and the second value being a total number of apparatuses in the plurality of further apparatuses~~from the another apparatus based on said authentication result~~; ~~and~~

a second counting unit operable to increment the count ~~a~~ of the total number of apparatuses ~~units of the another apparatus desiring~~ to receive the encrypted content ~~based on said number of additional units~~ by the first value when (i) the sum of the first value and the count of the total number of apparatuses is at most equal to the maximum value and (ii) the identification information of the another apparatus is already stored in said storage unit,

said second counting unit being operable to increment the count of the total number of apparatuses to receive the encrypted content by the second value when (i) the sum of the second value and the count of the total number of apparatuses is at most equal to the maximum value and (ii) the identification information of the another apparatus is not already stored in said storage unit.

3. (currently amended) An information processing apparatus according to Claim 1, further comprising:

an information updating unit operable to delete ~~said~~ the identification information stored in said storage unit and to reset ~~said~~ the count of the total number of apparatuses ~~units approved~~ to receive the encrypted content when said decryption key is changed.

4. (currently amended) A method for ~~transmitting~~ carrying out secure transmission of content from an information processing apparatus to another apparatus ~~via~~ over a network, said method comprising:

encrypting the content;

receiving ~~performing an~~ authentication ~~procedure with the~~ information from the another apparatus when the another apparatus requests permission to receive the encrypted content~~, said authentication procedure producing an authentication result~~;~~transmitting a decryption key for decrypting the encrypted content to the another apparatus based on said authentication result;~~

determining whether the authentication information is valid;

obtaining identification information of the another apparatus ~~based on said~~ from the authentication information when the authentication information is valid~~result~~;

determining whether the identification information of the another apparatus is already stored;

transmitting a decryption key to the another apparatus when the authentication information is valid, the decryption key being needed to decrypt the encrypted content;

incrementing a count~~ing~~ of a total number of apparatuses ~~units desiring~~ to receive the encrypted content ~~based on said~~ by one when the identification information of the another apparatus is not already stored and the count of the total number of apparatuses is less than a maximum value; and

storing ~~said~~ the identification information of the another apparatus when the identification information of the another apparatus is not already stored~~; andcontrolling a total number of units approved to receive the encrypted content based on said total number of units desiring to receive the encrypted content~~.

5. (currently amended) A recording medium having recorded thereon a program for ~~transmitting~~ executing a method for carrying out secure transmission of content from an information processing apparatus to another apparatus ~~via~~ over a network, said ~~program~~ method comprising:

encrypting the content;

receiving ~~performing an~~ authentication ~~procedure with the~~ information from the another apparatus when the another apparatus requests permission to receive the encrypted content~~, said authentication procedure producing an authentication result~~;~~transmitting a decryption key for decrypting the encrypted content to the another apparatus based on said authentication result;~~

determining whether the authentication information is valid;

obtaining identification information of the another apparatus ~~based on said~~ from the authentication information when the authentication information is valid~~result~~;

determining whether the identification information of the another apparatus is already stored;

transmitting a decryption key to the another apparatus when the authentication information is valid, the decryption key being needed to decrypt the encrypted content;

incrementing a count~~ing~~ of a total number of apparatuses ~~units desiring~~ to receive the encrypted content ~~based on said~~ by one when the identification information of the another apparatus is not already stored and the count of the total number of apparatuses is less than a maximum value; and

storing ~~said~~ the identification information of the another apparatus when the identification information of the another apparatus is not already stored~~; andcontrolling a total number of units approved to receive the encrypted content based on said total number of units desiring to receive the encrypted content~~.

6. (currently amended) An information processing apparatus for carrying out secure receiving of content from a first apparatus ~~via~~ over a first network and for carrying out secure transmission of the content to a second apparatus over a second network, said information processing apparatus comprising:

a first transmitting~~er~~ unit operable to transmit to the first apparatus a request for permission to receive the content;

a first authentication unit operable to perform a first authentication procedure with the first apparatus~~, said first authentication procedure producing a first authentication result~~;

a receiver operable to receive a first decryption key from the first apparatus when the first authentication procedure is successful ~~a first decryption key for decrypting the content based on said first authentication result;a second transmitter operable to transmit the content received from the first apparatus to a second apparatus via a second network;~~

a decryption unit operable to use the first decryption key to decrypt encrypted content received from the first apparatus;

an reencryption unit operable to reencrypt the decrypted content;

a second authentication unit operable to ~~perform a second~~ receive authentication ~~procedure with said~~ information from the second apparatus when a request for permission to receive the content is made from ~~said~~ the second apparatus and to determine whether the authentication information is valid~~, said second authentication procedure producing a second authentication result~~;~~a third transmitter operable to transmit a second decryption key to said second apparatus based on said second authentication result;~~

a first obtaining unit operable to obtain identification information of ~~said~~ the second apparatus ~~based on said second~~ from the authentication information when the authentication information is valid and to determine whether the identification information of the second apparatus is already stored in a storage unit~~result~~;

a second transmitting unit operable to transmit a second decryption key to the second apparatus when the authentication information is valid, the second decryption key being needed to decrypt the reencrypted content; and

a first counting unit operable to increment a count of a number of apparatuses ~~units desiring~~ to receive the reencrypted content ~~based on said~~ by one when the identification information of the second apparatus is not already stored in said storage unit and the count of the total number of apparatuses is less than a maximum value;

said ~~a~~ storage unit being operable to store ~~said~~ the identification information of said second apparatus when the identification information of the second apparatus is not already stored in said storage unit~~; anda controller operable to control a number of units approved to receive the content based on said number of units desiring to receive the content~~.

7. (cancelled)

8. (currently amended) An information processing apparatus according to Claim 6, further comprising:

a ~~fourth~~ third transmitting~~er~~ unit operable to transmit, ~~said~~ to the first apparatus, the count of the number of apparatuses ~~units desiring~~ to receive the content ~~to the first apparatus based on said first authentication result;~~

~~a second obtaining unit operable to obtain a number of additional units desiring to receive the content from said second apparatus based on said second authentication result; and~~

~~a second counting unit operable to count a total number of units of said second apparatus desiring to receive the content based on said number of additional units~~.

9. (currently amended) An information processing apparatus according to Claim 6, further comprising:

an information updating unit operable to delete ~~said~~ the identification information stored in said storage unit and to reset ~~said~~ the count of the number of apparatuses ~~units approved~~ to receive the reencrypted content when said second decryption key is changed.

10. (currently amended) A method for carrying out secure receiving of content ~~in an information processing apparatus~~ from a first apparatus ~~via~~ over a first network and for carrying out secure transmission of the content to a second apparatus over a second network, said method comprising:

transmitting to the first apparatus a request for permission to receive the content;

performing a first authentication procedure with the first apparatus ~~to obtain a first authentication result~~;

receiving a first decryption key from the first apparatus ~~a first decryption key for decrypting the content based on said~~ when the first authentication procedure is successful~~result~~;~~transmitting the content received from the first apparatus to a second apparatus via a second network;~~

decrypting, using the first decryption key, encrypted content received from the first apparatus;

reencrypting the decrypted content;

receiving ~~performing a second~~ authentication ~~procedure with said~~ information from the second apparatus when a request for permission to receive the content is made from ~~said~~ the second apparatus~~, said second authentication procedure producing a second authentication result~~;

determining whether the authentication information is valid;~~transmitting a second decryption key to said second apparatus based on said second authentication result;~~

obtaining identification information of ~~said~~ the second apparatus ~~based on said second~~ from the authentication information when the authentication information is valid ~~result~~;

determining whether the identification information of the second apparatus is already stored;

transmitting a second decryption key to the second apparatus when the authentication information is valid, the second decryption key being needed to decrypt the reencrypted content;

incrementing a count~~ing~~ of a number of apparatuses ~~units desiring~~ to receive the reencrypted content ~~based on said~~ by one when the identification information of the second apparatus is not already stored in said storage unit and the count of the total number of apparatuses is less than a maximum value;

storing ~~said~~ the identification information of ~~said~~ the second apparatus when the identification information of the second apparatus is not already stored~~; andcontrolling a number of units approved to receive the content based on said number of units desiring to receive the content~~.

11. (currently amended) A recording medium having recorded thereon a program for executing a method for carrying out secure receiving of content ~~in an information processing apparatus~~ from a first apparatus ~~via~~ over a first network and for carrying out secure transmission of the content to a second apparatus over a second network, said ~~program~~ method comprising:

transmitting to the first apparatus a request for permission to receive the content;

performing a first authentication procedure with the first apparatus~~ to obtain a first authentication result~~;

receiving a first decryption key from the first apparatus ~~a first decryption key for decrypting the content based on said~~ when the first authentication procedure is successful~~result~~;~~transmitting the content received from the first apparatus to a second apparatus via a second network;~~

decrypting, using the first decryption key, encrypted content received from the first apparatus;

reencrypting the decrypted content;

receiving ~~performing a second~~ authentication ~~procedure with said~~ information from the second apparatus when a request for permission to receive the content is made from ~~said~~ the second apparatus~~, said second authentication procedure producing a second authentication result~~;

determining whether the authentication information is valid;~~transmitting a second decryption key to said second apparatus based on said second authentication result;~~

obtaining identification information of ~~said~~ the second apparatus ~~based on said second~~ from the authentication information when the authentication information is valid ~~result~~;

determining whether the identification information of the second apparatus is already stored;

transmitting a second decryption key to the second apparatus when the authentication information is valid, the second decryption key being needed to decrypt the reencrypted content;

incrementing a count~~ing~~ of a number of apparatuses ~~units desiring~~ to receive the reencrypted content ~~based on said~~ by one when the identification information of the second apparatus is not already stored in said storage unit and the count of the total number of apparatuses is less than a maximum value;

storing ~~said~~ the identification information of ~~said~~ the second apparatus when the identification information of the second apparatus is not already stored~~; andcontrolling a number of units approved to receive the content based on said number of units desiring to receive the content~~.

12. (new) An information processing apparatus according to Claim 1, wherein the authentication information includes first authentication information and second authentication information, and said authentication unit includes:

a first authentication subunit operable to receive the first authentication information from the another apparatus when the another apparatus requests permission to receive the encrypted content, and to determine whether the first authentication information is valid; and

a second authentication subunit operable to transmit a request for the second authentication information to the another apparatus when the first authentication information is valid, to receive the second authentication information from the another apparatus, and to determine whether the second authentication information is valid;

said transmitting unit being operable to transmit the decryption key to the another apparatus when the second authentication information is valid.

13. (new) An information processing apparatus according to Claim 6, wherein the authentication information includes first authentication information and second authentication information, and said second authentication unit includes:

a first authentication subunit operable to receive the first authentication information from the second apparatus when the second apparatus requests permission to receive the content, and to determine whether the first authentication information is valid; and

a second authentication subunit operable to transmit a request for the second authentication information to the second apparatus when the first authentication information is valid, to receive the second authentication information from the second apparatus, and to determine whether the second authentication information is valid;

said second transmitting unit being operable to transmit the second decryption key to the second apparatus when the second authentication information is valid.